WE CLAIM:

1. A system for controlling access to a platform, the system comprising:

a platform having a software services component and an interface component, the interface component having at least one interface for providing access to the software services component for enabling application domain software to be installed, loaded, and run in the platform; and

an access controller for controlling access to the software services component by a requesting application domain software via the at least one interface, the access controller comprising:

an interception module for receiving a request from the requesting application domain software to access the software services component; and

a decision entity for determining if the request should be granted; and

wherein the requesting application domain software is granted access to the software services component via the at least one interface if the request is granted.

2. The system according to claim 1, wherein the decision entity is a security access manager, the security access manager holding access and permission policies.

3. The system according to claim 2, wherein:

the request includes an identification of the requesting application domain software; and

the security access manager includes a collection of records of approved requesting application domain software for use in determining if the request should be granted to the requesting application domain software based on the identification.

4. The system according to claim 3, wherein:

the collection of records comprises an access control collection;

the security access manager contains an associated permission collection; and

the associated permission collection is used to determine if the request should be granted for a requesting application domain software included in the access control collection.

5. The system according to claim 2, wherein the security access manager comprises a decision cache for maintaining a record of requests by application domain software for determining if a permission decision has previously been granted to the requesting application domain software.

6. The system according to claim 2, wherein:

the security access manager has a record of requesting application domain software; and

the security access manager determines if the request should be granted based on an identification stored in the record.

7. The system according to claim 2, wherein, if the request is denied, a reject message is sent to the requesting application domain software by the interception module.

8. The system according to claim 2, wherein the application domain software comprises non-native application domain software.

9. The system according to claim 8, wherein the non-native application domain software comprises Java application software.

10. The system according to claim 1, wherein the application domain software comprises native application software.

11. The system according to claim 1, wherein the interface component comprises a middleware services layer.

12. The system according to claim 2, wherein the platform comprises a platform for a mobile terminal for a wireless telecommunications system.

13. The system according to claim 1, wherein the decision entity is the interception module.

14. The system according to claim 13, wherein:

the request includes an identification of the requesting application domain software; and

the interception module includes a collection of records of approved requesting application domain software for use in determining if the permission request should be granted to the requesting application domain software based on the identification.

15. The system according to claim 14, wherein the interception module comprises a decision cache for maintaining a record of application-software identifiers grouped by native platform service for determining if a permission decision has previously been granted to the requesting application domain software.

16. The system according to claim 13, wherein:

the interception module has a record for each platform service of the platform; and

the interception module determines if the request should be granted based on an identification stored in the record.

17. The system according to claim 13, wherein the application domain software comprises non-native application software.

18. The system according to claim 13, wherein the application domain software comprises native application software.

19. The system according to claim 1, further comprising:

a system access module; and

wherein the system access module is adapted to update the interception module with information for use by the interception module to determine whether to grant or deny the request.

20. The system according to claim 19, wherein updates by the system access module occur periodically.

21. The system according to claim 19, wherein updates by the system access module occur in response to an update request.

22. A method of controlling access to a platform having a software services component and an interface component, the interface component having at least one interface for providing access to the software services component for enabling application domain software to be installed, loaded, and run on the platform, the method comprising:

receiving a request from a requesting application domain software to access the software services component;

determining if the request should be granted; and

if the request is granted, granting access to the requested software services component via the at least one interface.

23. The method according to claim 22, wherein:

the request includes an identification of the requesting application domain software; and

a collection of possible requesting application domain software is used in the step of determining if the request should be granted.

24. The method according to claim 23, wherein the collection comprises:

an access control collection; and

wherein the determining step comprises accessing the access control collection.

25. The method according to claim 22, wherein the determining step comprises determining if a decision has previously been granted to the requesting application domain software.

26. The method according to claim 22, wherein:

a record is stored for each platform service of the platform; and

the determining step includes determining if the request should be granted to the requesting application domain software based on an identification stored in the record.

27. The method according to claim 22, comprising:

if the request is denied, sending a reject message to the requesting application domain software.

28. The method according to claim 22, wherein the application domain software comprises non-native application software.

29. The method according to claim 28, wherein the non-native application domain software comprises Java application software.

30. The method according to claim 22, wherein the application domain software comprises native application software.

31. The method according to claim 22, wherein the platform comprises a platform for a mobile terminal for a wireless telecommunications system.

32. The method according to claim 22, further comprising updating information used to determine whether to grant or deny the request.

33. The method according to claim 32, wherein the step of updating is periodically repeated.

34. The method according to claim 32, wherein the step of updating occurs in response to an update request.

35. A system for controlling access to a platform for a mobile terminal for a wireless telecommunications system, the system comprising:

a platform having a software services component and an interface component, the interface component having at least one interface for providing access to the software services component for enabling non-native application software to be installed, loaded, and run on the platform; and

an access controller for controlling access to the software services component by the non-native application software via the at least one interface, the access controller including:

an interception module for receiving a request from the non-native application software to access the software services component; and

a decision entity for determining if the request should be granted; and

wherein the non-native application software is granted access to the software services component via the at least one interface if the request is granted.

36. The system of claim 35, wherein the decision entity is the interception module.

37. The system of claim 35, wherein the decision entity is a security access manager.

38. The system according to claim 35, wherein the at least one interface comprises a middleware services layer.

39. The system according to claim 35, wherein the non-native application software comprises Java application software.

40. The system according to claim 35, wherein native application software may be loaded, installed, and run on the platform.